SWB SPECIFICATION COMMENTS AND RESPONSES

Hard Drive Software Write Block Tool Specification & Test Plan Version 3.0

1. Purpose

The specification *Hard Drive Software Write Block Tool Specification & Test Plan Draft Version 3.0 May 14, 2003* was posted on the Computer Forensics Tool Testing (CFTT) website (http:/www.cftt.nist.gov/) and users were notified that it was available for review. This report documents the comments, responses, and other changes made to create the final version (September 1, 2003).

Comments are grouped according to common threads and the related paragraphs in the document. Comments are in *italics* and the response follows in roman typeface.

1.1 Requirements

1. *First, I think we need to come up with a new name for these categories. Optional Requirement just isn't right. Maybe Optional Features, but you just can't have an optional requirement.*

The categories were renamed to:
Requirements for Mandatory Features and Requirements for Optional Features

2. *As for the tool logging disk drive model, serial number, etc... I don't really see a need for this in a write blocking tool. I mean, we can all come up with extra goodies we would like to see every tool have, but at what point do we stay enough. We could also say we want a write blocker to automatically hash upon startup, and hash upon exit.....and all could be "nice" features, but should they really be included in the specification.*

Two nice to have but not really necessary requirements were removed:
SWB-RO-04 logging and SWB-RO-05 status of last command.

3. *Section 6.2 Optional requirements: It would be nice for the program to have the capability of showing the drives (and sizes) it identifies, before the user is forced to choose one. This is especially useful when IDE's and SCSI's are mixed, as the drive numbers may not be assigned as expected and the user might instruct the program to block the wrong drive number.*

No action taken. This is nice to have but not essential.

4. *Section: 8.2.2 N Drives: the indication (even though you stated simple SCSI adapter) of 7 SCSI drives is somewhat outdated. Almost all top of the line SCSI adapters today can handle 15 drives. This change should be considered.*

Text changed to allow for up to 15 drives.

1.2 Test Methodology

5. *I couldn't find any obvious holes in the s/w write blocker draft doc, however, the tests seem to rely on the BIOS's return code only. Considering how many BIOS'es there are in existence, I feel that a slightly greater level of assurance could be achieved by using a different platform to perform an MD5 hash computation of the test HDD before and after a test cycle to provide some measure of assurance as to whether the hdd conts have changed or not. For example, prior to the tests, booting with a bootable Linux-CD (that does not mount any hard disks) perform "dd if=/dev/hda |md5sum " would perform an MD5 hash sum of the entire hdd (dd will state the sector count) Perhaps something like this could be inserted at pre/post test points. What do you think?*

The test methodology was changed to add a SHA1 hash comparison before and after testing of drives used.

1.3 Scope of Specification

6. *The draft on the Hard Drive Software Write Block Tool Specification & Test Plan Version 3.0 is very comprehensive for one method of write blocking hard drives with software. Page 1 of 24, 3 Scope, lines 39-41, describes the scope of the specification: "The scope of this specification is limited to software tools that protect a hard drive attached to a PC from unintended modification. The specifications are general and could be adapted to other software write blocking tools. However, actual testing is currently confined to tools that protect drive access through the interrupt 0x13 BIOS interface of a PC."*

   Page 2 of 24, 5.1 Hard Drive Attachment and Access, lines 33-36, describes Windows XP (and other OSs) using device drivers to access hard drives, demonstrating NIST's understanding of the differences between DOS and "more complex operating systems" access to hard drives. As there are other methods and technologies available to protect hard drives with software, other than DOS interrupt 0x13, the title or subtitle of the draft could be altered to reflect the very specific scope of this test plan.

The scope was changed to clarify that the current test plan is for interrupt 0x13 based write blockers. A statement was added that if software write blocking tools other than interrupt 0x13 based tools are tested (e.g., windows device driver based tools), an additional test plan, specific to the type of tool tested will be developed and published as an addendum to this document.

The document title was changed from “Hard Drive Software Write Block Tool Specification & Test Plan Version 3.0” to “Software Write Block Tool Specification & Test Plan Version 3.0.”

1.4 Other Changes

The following changes were also made to the document:

1. The Requirements and test assertions were renumbered.
2. A list of interface definitions was added to section 5.
3. An explicit list of optional features added to section 6.2.
4. Clarification that all 256 possible interrupt 0x13 commands are tested was added to section 8.2.1.
5. Minor adjustment were made to assignment of commands to categories in section 8.2.1.
6. A text summary of each test case was added to section 9.
7. A requirement was added for the tool to optionally protect drives during boot and shutdown.
8. Two test cases were inserted to cover protecting drives during boot and shutdown.
9. One test case corresponding to the deleted return status requirement was removed.
10. Test protocols were revised to account for above changes in requirements and test cases.